



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/774,720	02/09/2004	Xavier Boyen	ID-5	9562
36532	7590	11/05/2010	EXAMINER	
Treyz Law Group 870 Market Street, Suite 984 San Francisco, CA 94102			DOAN, TRANG T	
			ART UNIT	PAPER NUMBER
			2431	
			MAIL DATE	DELIVERY MODE
			11/05/2010	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/774,720

**Applicant(s)**

BOYEN, XAVIER

**Examiner**

TRANG DOAN

**Art Unit**

2431

**Period for Reply** -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 31 August 2010.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 1-12, 18 and 19 is/are allowed.
- 6) ☒ Claim(s) 13-17 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 09 February 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB-06)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

1. This action is in response to the amendment filed on 08/31/2010.
2. Claims 1-19 are pending for consideration.

***Response to Arguments***

3. Applicant's arguments with respect to the rejection under 35 U.S.C. 112, 2<sup>nd</sup> paragraph are persuasive. Therefore, the rejection under 35 U.S.C. 112, 2<sup>nd</sup> paragraph, has been withdrawn.
4. Applicant's arguments filed on 08/31/2010 have been fully considered but they are not persuasive.

Applicant argues on page 13 of the Remarks that Gentry does not disclose using an IBE private key to compute a decommitment that corresponds to a commitment to a secret value. Examiner respectfully disagrees with Applicant's arguments. Gentry does disclose using an IBE private key to compute a decommitment that corresponds to a commitment to a secret value (Gentry: column 5 lines 4-22). Examiner notes, a third party private key generator recited in the above cited column is used to generate IBE private key. Gentry further discloses using the IBE private key to compute a public key (i.e., commitment) and private key (i.e., decommitment) (Gentry: column 5 lines 10-12: PKG determines the first entity's private key Sa...provide private key to the first entity and column 6 lines 64-66: generator g is used to create public keys Pa, Pb).

Applicant further argues on pages 13-14 of the Remarks that Deng does not disclose using a symmetric key that is based on an IBE private key to encrypt a

commitment or a decommitment. Examiner respectfully disagrees with Applicant's arguments. Deng does disclose using a symmetric key that is based on an IBE private key to encrypt a commitment or a decommitment (Deng: column 6 lines 55-57: encrypting a key k using a symmetric key cryptosystem). Examiner notes, the key K cited in the above column can either be a public key (i.e., commitment) or private key (i.e., decommitment). Therefore, Deng does disclose using a symmetric key to encrypt a commitment or a decommitment.

### ***Claim Objections***

5. Claims 14-15 are objected to because of the following informalities:

The limitation "concatenating the decommitment and the message" recited in claim 14 should be changed to "concatenating the decommitment and a message".

The limitation "concatenating an IBE public key with the message" should be changed to "concatenating an IBE public key with a message".

Appropriate correction is required.

### ***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 13-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gentry et al. (US 7353395) (hereinafter Gentry) in view of Deng et al. (US 6910129) (hereinafter Deng).

Regarding claim 13, Gentry discloses a method of signing and encrypting a message M comprising: obtaining an identity-based-encryption (IBE) private key of a user (Gentry: column 9 lines 9-11: system also includes a private key generator...generates...private keys); using the IBE private key to compute, with computing equipment, a commitment to a secret value and a corresponding decommitment (Gentry: column 5 lines 5-27: The public key Pa is the commitment. The secret value is a non-interaction shared secret Sab. The private key Sa is the decommitment).

Gentry discloses using a symmetric key that is based on the IBE private key (Gentry: column 6 lines 29-31 and column 7 lines 16-18). Gentry does not disclose using a symmetric key to encrypt, with computing equipment, at least one of the commitment and the decommitment. However, Deng discloses using a symmetric key that is based on the IBE private key to encrypt at least one of the commitment and the decommitment (Deng: column 6, lines 55-57: using a symmetric key to encrypt a key K (i.e., private key)). Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to have included in Gentry the feature of Deng as discussed above to achieve confidentiality when sending a private key over a public

network. The symmetric key is used in this situation to protect the private key from exposing it to unauthorized users.

Regarding claim 14, Gentry in view of Deng further discloses wherein using the symmetric key to encrypt comprises: concatenating the decommitment and the message (Deng: column 6, lines 55-57: encrypted message containing original message  $m$  and a key  $k$  using a symmetric key; and column 12 lines 19-46); and using the symmetric key to encrypt the concatenated decommitment and message (Deng: column 6, lines 55-57; and column 12 lines 19-46).

Regarding claim 15, Gentry in view of Deng further discloses wherein using the symmetric key to encrypt comprises: concatenating an IBE public key with the message and the decommitment (Deng: column 12 lines 19-46); and using the symmetric key to encrypt the concatenated IBE public key, decommitment, and message (Deng: column 12 lines 19-46).

Regarding claim 16, Gentry in view of Deng further discloses wherein computing the decommitment comprises performing multiplication on an elliptic or hyperelliptic curve (Gentry: column 7 lines 50-55: an elliptic curve).

Regarding claim 17, Gentry in view of Deng further discloses computing the symmetric key that is based on the IBE private key by performing a bilinear pairing calculation on an elliptic or hyperelliptic curve (Gentry: column 4 lines 28-41).

***Allowable Subject Matter***

8. Claims 1-12 and 18-19 are allowed.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/  
Examiner, Art Unit 2431

/William R. Korzuch/  
Supervisory Patent Examiner, Art Unit 2431